HISPOL 002.0

The United States House of Representatives General Information Security Guidelines for Protecting Systems from Unauthorized Use

CATEGORY: General Information Security

ISSUE DATE: **February 4, 1998**
Revised Date: **October 28, 2003**

The United States House of Representatives
Committee on House Administration

Title: United States House of Representatives – General Information Security Guidelines for Protecting Systems from Unauthorized Use

Number: HISPOL 002.0

Category: General Information Security

Date: February 4, 1998
Revision: October 28, 2003

Status: Approved – Committee on House Administration

Purpose:

The purpose of the United States House of Representatives – General Information Security Guidelines for Protecting Systems from Unauthorized Use is to provide House and Administrative offices with a policy governing general information security requirements for using House computing and network resources. This policy is also applicable to vendors and contractors that install, maintain, support, and otherwise have access to House network and information systems.

This document outlines the security rules, regulations, and expectations according to the various roles that House users, contractors, system programmers, administrators, and managers have in the information security area.

Audience:

This document has relevance to all House Offices and provides a policy governing general information security requirements for using House computing and network resources. This policy is also applicable to vendors and contractors that install, maintain, support, and otherwise have access to House network and information systems.

References:

U.S. House of Representatives Information Systems Security Program

External References:

House Code of Official Conduct

Committee on House Administration Resolution – Electronic Communications - July 31, 1996

Committee on House Administration Resolution – World Wide Web Sites - July 31, 1996

Table of Contents

1.0 INTRODUCTION

The purpose of this policy is to provide a comprehensive set of guidelines for the responsible and secure use of U.S. House of Representatives (House) information systems and network resources. The secure use of these resources requires individual responsibility, knowledgeable users, and an effective security program to ensure a safe and secure computing environment. In addition to the human aspect of the security program, technical solutions will continue to be implemented for both the perimeter (i.e., firewall) and internal host protections. The overall strategy of the House Information Systems Security Program is to protect all House systems against internal and external threats via the effective implementation of technical solutions and personnel policies.

1.1 General Information Security Guidelines

General Information Security Guidelines are part of a comprehensive program to provide information security at the House. They represent an approach whereby each employee is accountable for his/her actions and is subsequently responsible for information systems security. Because the procedures and technical controls necessary to address all security concerns cannot always be implemented in a cost-effective manner, General Information Security Guidelines establish ethical and practical standards predicated on the concept that knowledgeable employees are the foundation of a successful information security program.

General Information Security Guidelines identify to the user community their roles and responsibilities with regard to protecting information. The guidelines imply that a proactive approach be taken to ensure that employees are: (1) alert to the latest threats and vulnerabilities, (2) knowledgeable of security policies and procedures, and (3) aware of their responsibility to report incidents to the proper authorities. Employees are also called upon to take initiative and accept responsibility for safeguarding information systems resources. These guidelines apply to all employees of the House as well as contractor personnel supporting House systems.

The primary threats to information security have typically been from insiders who access information and systems on a routine basis. With the proliferation of distributed networks, public access systems including the Internet and dial-in capability, threats now include those from external sources. Within all computing environments, technical controls such as firewalls are not enough to ensure an adequate and comprehensive information systems security program. Management controls such as password management and physical security must be used to augment technical controls.

1.2 Overall Strategy for General Information Security Guidelines

The implementation of information systems security at the House focuses not only on the protection of information and network systems but also on the protections necessary for safeguarding the information itself. Therefore, the General Information Security Guidelines address all forms of computer generated information including hardcopy and electronic formats. NOTE: This policy does not address or pertain to records retention.

General information security guidelines:

- must be included in security planning for both general support systems and major application systems,
- establish personnel, technical and physical controls,
- set standards and expectations,
- establish work procedures, automated control mechanisms, and capabilities for system backup and recovery,
- implement an enforcement mechanism.

1.3 Intent of This Document

This document has been developed to:

- be used as part of daily operations to ensure an adequate level of security exists for information systems used throughout the House,
- explain the general requirements for information systems security that can be used to develop security for general support systems and major applications. As such, this policy can be augmented as required by specific guidance in the form of Office policy and additional House policies (HISPOLs) and procedures (HISPUBs), which will be developed, approved, and disseminated as needed.

2.0 REQUIREMENTS FOR GENERAL INFORMATION SECURITY GUIDELINES

As stated in the previous section, the General Information Security Guidelines are designed to address both general support systems and major applications. The definitions are as follows:

A ***general support system*** is defined as…

…an interconnected set of information resources under the same direct management control which shares common functionality. A system normally includes hardware, software, information, data, applications, communications, and people.

An in-office local area network (LAN), House-wide backbone, communications (voice and data) network, data processing center, and shared information processing service organization are all examples of general support systems.

A ***major application*** is defined as…

…an application that requires special attention to security due to the risk and magnitude of harm resulting from the loss, misuse or unauthorized access to or modification of the information in the application.

Examples of major applications in use at the House are the Federal Financial System (FFS) and the House Messaging System.

2.1 Existing Systems

For existing systems, the guidelines created for the system must correspond to and support technical controls (e.g., if the rules dictate that a eight character password comprised of numbers and characters is required, the rules must state this requirement).

2.2 Policy Rules

Policy and procedural rules must address the following environments:

- work at home,
- authorized telecommuting,
- remote access,
- connections to the Internet,
- use of copyrighted works,
- proper use of House equipment,
- assignment and limitation of system privileges,
- separation of duties,
- individual accountability,
- information dissemination,
- access control to and from other systems, including limitations on external access.

2.3 Policy Rule Limitations

Policy and procedural rules must include limitations on:

- modifying data,
- searching databases,
- divulging information.

2.4 Policy Rules and Training

The rules developed for each system must be addressed as part of the security training provided for each general support system and major application.

2.5 Consequences

Consequences must be written into various rules so that House employees, contractor personnel, or any other authorized persons using House systems are adequately advised.

3.0 GENERAL PRINCIPLES

The following principles apply to House employees and contractor personnel either using or providing support for various House information systems. Section 3.1 applies to general users of House systems. Section 3.2 applies to certain unique users and provides specific principles over and above Section 3.1. Guidance on specific procedures unique to specialized systems will be provided as needed. Written guidance cannot be generated for every system contingency; therefore, personnel may sometimes have to go beyond stated principles and use their best judgment to guide their actions. Personnel must understand that many of the principles are based on Federal law and the House Code of Official Conduct. As such, there are consequences for non-compliance with the "Principles of Behavior." Refer to Section 4.4 for consequences for non-compliance.

Guidance in this and other documents may be categorized under the headings of either *"must"* or *"recommendation."* Items designated as *"must"* are considered requirements because their absence can adversely affect the security posture of the entire House. Items designated as "must" will be enforced. Items under the designation of *"recommended"* are considered prudent security practices but will not be enforced by the House. Employing authorities may require adherence to recommended items to better protect their individual information systems.

3.1 Principles of Behavior for General Use of House Information Systems

Official Business	House information systems may not be used contrary to public law, House Rules, and Committee on House Administration regulations.
Access	Access and use only information for which they have official authorization.
Accountability	Be accountable for their own actions and responsibilities related to information and information systems entrusted to them.
Confidentiality	Protect information from unauthorized disclosure.
Integrity	Protect information from unauthorized, unanticipated, or unintentional modification, including the detection of such activity.
Availability	Protect information so that it is available on a timely basis to meet mission requirements or to avoid substantial losses.

Password and User IDs	Protect information security through effective use of user IDs and passwords.
Hardware	Protect computer equipment from damage, abuse, theft, sabotage, and unauthorized use.
Software	Use appropriate software in a safe manner so that software is protected from damage, abuse, theft, sabotage, and unauthorized replication or use (copyright infringement).
Awareness	Stay alert to security policies, requirements, procedures, and issues.
Reporting	Report security violations, incidents, and vulnerabilities to proper authorities.

Official Business

House information systems may not be used contrary to public law, House Rules, and Committee on House Administration regulations.

Employees are expected to use House equipment, systems, and information to carry out their official duties. At the same time, employees must remember that public service is a public trust – information gained through employment at the House must be used in accordance with applicable laws, rules of the House, and regulations of the Committee on House Administration.

Employees must:

- follow House guidelines regarding the use of information systems, recognizing that incidental personal use is permitted only when such use is negligible in nature, frequency, time consumed, and expense,
- not use government information for private gain (e.g., an employee of a procurement organization must not use knowledge of a pending contract award as a basis for purchasing stock in the vendor's company),
- avoid the appearance of impropriety,
- not initiate or propagate harassing e-mail, chain letters, or other inappropriate use of electronic communication systems,
- not send electronic mail that causes any House user to be flooded with unwanted, irrelevant, or inappropriate electronic messages which could be construed as spam,
- not conduct system risk assessments, vulnerability scans, or penetration tests without notification to the Chief Administrative Officer (CAO) House Information Resources

(HIR) Information Systems Security Office, and prior written authorization, including a description of the requested action, from their Employing Authority, which shall be filed with the Information Systems Security Office,

- not use information in a way that would adversely affect public confidence in the integrity of the House as a body.

NOTE: House information resources are assets, owned by the House and its Members. Offices are responsible for determining their own policies for in-office equipment, including equipment used to access or process electronic information. All such in-office policies must be in compliance with House information systems security policies and must not change the intent of these policies. House Offices are responsible for following and enforcing guidelines set forth in the House information security policies.

Access — Employees shall access and use only information for which they have official authorization.

The concepts of *need-to-know* and *least privilege* are important tenets of information access security. *Need-to-know* means only authorized individuals who have a demonstrated need to access information will have access to such House information. *Least privilege* means each information user is only provided rights necessary to access information or services needed to carry out job responsibilities (e.g., multiple logins for system administration, access to financial systems, etc.). These concepts apply to non-public information (e.g., procurement, data, employee records, etc.) and systems.

Employees must:

- follow established procedures for accessing information, including use of User Identification (ID), user authentication, passwords, and other physical and logical control measures,

- follow established channels for requesting and disseminating information (Do not ask another employee with different or higher access privileges to get information for you.),

- not give information to other employees or outside individuals who do not have authorization to it,

- not attempt to perform actions or processing on a computer for which they do not have authority, or which exceeds their authority, including system risk assessments, vulnerability scans, or penetration tests,

- not store sensitive files on a fixed hard drive if access to that particular computer cannot be limited to authorized users.

- ***It is recommended that employees***:

- set PCs to lockup (i.e., screensaver passwords) after a specified amount of idle time,

- take measures to limit who can access files and printed information on personal computers – only people who need the information should be able to get it.

Accountability

House Offices and their employees are accountable for their actions and responsibilities related to information resources entrusted to them.

Organizations can only build partial accountability through structure and procedural controls. To a much greater extent, the benefits of accountability depend on the trustworthiness of each employee. It is each employee's responsibility to behave ethically, to develop technical proficiency, and to stay informed about issues and systems related to his/her job. Employees must approach information security with a spirit of cooperation and responsibility.

Employees must:

- agree to and participate in accountability controls, such as automated transaction logging and manual logs,

- acknowledge actions and accept responsibility for correcting errors and rectifying problems,

- not attempt to override internal controls,

- be alert to threats and vulnerabilities to information security from both internal and external sources,

- sign and adhere to the Affirmation of Non-Disclosure Statement (HISFORM-008.0) if required by the job function.

It is recommended that employees:

- ensure that no single person has sole access or control over sensitive information resources,

- prevent others from using his/her accounts by using procedures such as:

    - logout when leaving the vicinity of the terminal or PC,
    - set a password on automatic screen savers,
    - password-protect or encrypt (using two or more public keys) sensitive files and software.

♦ help remedy security breaches.

Confidentiality

Employees must protect the confidentiality of sensitive information from disclosure to unauthorized individuals or groups.

Access to sensitive information must be restricted to authorized individuals who need it to conduct their jobs. This entails not only refraining from intentional disclosure but also using measures to guard against accidental disclosure. Employees are responsible for both. When an employee changes positions or terminates employment with the House, he/she is still obligated to protect the confidentiality of information.

The principles here do not address National Security Information (NSI). NSI is information relative to the national defense or foreign relations of the United States and requires special protection provisions. Member and Committee offices that have a need to process NSI should contact the applicable security organization for guidance.

Employees must:

♦ be aware of the sensitivity levels of information being accessed and protect it accordingly,

♦ protect the following information:

- ***Confidential Business Information (CBI)*****:** any procurement, proprietary, financial, commercial, and information afforded protection from disclosure by statutes applicable to the House (e.g., network infrastructure information, telephone credit card numbers, contract proposals, etc.),

- ***Confidential House or Employing Authority Information (CHI)*****:** personal information about individuals contained in "systems of record," any collection of records on individuals from which information is retrieved by the individual's names or other personal identifiers (e.g., medical history, work performance, etc.).

- To ensure the accuracy of appropriately determining CBI and CHI, please refer to HISPUB 008, Determining Information Sensitivity.

♦ not store or transmit sensitive information on any public access system such as e-mail or via the Internet without protective measures (e.g., encryption). (Encryption is software or hardware that give users the capability to convert/recover data that has been put into an unreadable format while it is in transit or in storage. Contact the HIR Information Systems Security Office or your TSR for details.),

♦ not allow unauthorized personnel access to facilities and resources that store or process sensitive information,

- dispose of media (e.g., diskettes, disk drives, etc.) in accordance with in-office and/or approved procedures (note: media returned to CAO is properly disposed of to preserve confidentiality of the member/committee/House office),

- not leave paper copies of sensitive information unattended,

- limit information on a need-to-know basis or provide sanitized versions of sensitive House network diagrams to Contractors which will exclude House IP address allocation and House server naming schema.

It is recommended that employees:

- not allow sensitive data to remain on their computer screen or be visible by someone who is not authorized to view the data,

- protect all computer generated print outs and media (e.g., disks, tapes, etc.) containing sensitive data,

- mark CBI and CHI sensitive media accordingly,

- when testing systems use simulated rather than live data.

Integrity — Employees must protect the integrity and quality of information.

Employees must protect both the integrity and quality of information. Information integrity can be corrupted by intentional alteration or accidental damage. Information is of high quality if it is accurate, complete, and up-to-date. Information quality is dependent on its source; it must be correct when created and maintained in that same quality.

Employees must:

- protect information against viruses and similar malicious code by using virus detection and correction (anti-virus) software. (Anti-virus software can be configured to stay resident on your system and scan for the presence of computer viruses. Anti-virus software is provided by the House, contact your TSR for details.)

It is recommended that employees:

- review information as it is collected, generated, and used to make sure it is accurate, complete, and up-to-date,

- prevent unauthorized alteration, damage, destruction, or tampering of information (e.g., use effective passwords, write protect files and programs on disks, keep area clear of food and drinks, etc.),

- use protective measures to ensure against accidental loss of information integrity (e.g., backups, etc.),

- avoid using "unofficial" software, such as shareware and public domain software,

- take appropriate training before using a system to learn how to correctly enter and change the data,

- discontinue use of a system at the first sign of a virus infection and seek technical assistance from the HIR Information Systems Security Office.

Availability

Employees should protect the availability of information and systems.

Computer systems and media (e.g., diskettes, hard drives, tapes, etc.) should be protected from environmental factors such as fire, water, heat, and food spills. They should also be protected from theft, unauthorized alteration, and careless handling.

With preparation, employees can minimize the impact of contingencies such as natural disasters, loss of information, and disclosure of information. It is each employee's responsibility to be rehearsed in recovery activities associated with their systems.

It is recommended that employees:

- use physical and logical protective measures to prevent loss of availability of information and systems, such as:

    - perform and protect good backups, never storing backups in the same location as primary copies,
    - use Uninterruptable Power Supplies (UPS) on fileservers to ensure no loss of data in the event of power outage,
    - protect media – disks, tapes, and hard copy reports – that store information,
    - maintain an inventory of files and programs.

- store backups in a metal cabinet where they will be safe from fire and water damage,

- keep hardware away from direct sunlight or extreme temperatures,

- take appropriate action to restore availability when information or systems become unavailable due to disaster, damage, or unplanned shutdown.

Passwords

Protect information through the effective use of user IDs and passwords.

User IDs and passwords are the most widely used security controls for automated information systems. If used properly, they are quite effective in preventing accidental or negligent damage and access. (Protection from hackers usually requires more sophisticated techniques.) For user IDs and passwords to be effective, all House employees, privileged users, and contractors/vendors must follow guidelines for constructing and using them.

Employees must:

- protect information through effective use of user IDs and passwords,
- construct effective passwords that are a minimum of eight characters in length and:
  - do use a combination of alpha and numeric characters,
  - avoid obvious ones like variations of your name, address, Social Security Number, hobby, or personal attributes,
  - do not use a readable word (i.e., from a dictionary) in any language,
  - do not use words associated with offices, committees, Capitol Hill, etc.
- change passwords frequently - at least every 90 days or immediately when they may have been disclosed,
- follow login procedures without automating steps that insert passwords (i.e., ensure that you manually enter your ID and password),
- never share your user ID or password without good reason (e.g., unexpected absence, critical information access, etc.) since system audit logs identify users based on user IDs,
- not attempt to guess someone else's ID or password (Guessing on the part of a legitimate user would falsely indicate suspicious activity to the system's audit function.),
- report unauthorized attempts to access your system to your office manager or a member of the security staff,
- when setting up new systems, make sure all accounts have passwords and change passwords on default accounts (e.g., supervisor, maintenance, etc.).

It is recommended that employees:

- use a password on PC power up and screensaver options if applicable,

- ♦ enter a password only when no one else is present or at least watching your entry on the keyboard,

- ♦ safeguard your password – commit it to memory, do not write it down or post it, do not store it on a computer,

- ♦ when changing your password, use one that you have not used in the past,

- ♦ not use the same ID or password on multiple systems.

Hardware

Protect computer equipment from damage, abuse, theft, sabotage, and unauthorized use.

Each employee has a duty to protect and conserve House property either owned or under evaluation, including information processing equipment. Employees have access to many kinds of office and computing equipment and must handle such equipment carefully to protect against hazards. Further, employees must prevent problems by performing maintenance regularly. Backup and recovery plans and mechanisms for general support systems and major applications will be addressed by separate documentation.

Employees must:

- ♦ protect computer equipment from damage, abuse, theft, sabotage, and unauthorized use (i.e., by locking office doors, permitting only authorized personnel access, etc.),

- ♦ follow established procedures by getting a HIR property pass (HISFORM 017.0) when removing equipment from House premises, if appropriate.

It is recommended that employees:

- ♦ protect computer equipment from hazards, such as:

    - extreme temperatures,
    - water and fire,
    - electrical storms,
    - static electricity,
    - spills from food and drink,
    - dropped objects,
    - dust and dirt,
    - combustible materials by using measures such as static mats, surge suppressors, UPS, etc.

- ♦ keep an inventory of all equipment assigned to them,

- when equipment requires repair by service personnel, ask to see the service person's identification and keep records of the work performed,

- disconnect or deactivate modems when they are not in use.

Software **Use appropriate software in a safe manner so that it is protected from damage, abuse, theft, sabotage, and unauthorized replication or use (copyright infringement).**

Computer users must utilize only appropriate software on House-provided computer systems and must protect those systems from viruses. Software downloaded from the Internet presents the greatest potential vulnerability associated with virus infections to House computing systems.

Employees must:

- use the House-provided or an equivalent current anti-virus program to scan software prior to installing on any office computers,

- not use, install, or download software, other than Employing Authority-approved network operating systems and diagnostic programs, that allows an individual workstation to act as a server permitting other users to connect to that workstation and share files,

- not use, install, or download hacker or cracker software or scanning tools on House computer systems without notification to the CAO HIR Information Systems Security Office, and prior written authorization from their Employing Authority, which shall be filed with the Information Systems Security Office.

It is recommended that employees:

- use software in a safe manner that protects software from damage and abuse,

- use only authorized software. Install shareware or public domain software only in accordance with your office policies,

- not alter software, or allow another person to do so, except as authorized,

- consider maintaining up-to-date, safeguarded back-ups. Store back-ups in a different location from the primary copy, preferably under lock and key.

It is the policy of the House to comply fully with all copyright laws pertaining to computer software. Accordingly, the House prohibits the illegal duplication or use of any software or related documentation. If appropriate, sign and register software license agreements with the vendor within a few days of receipt.

Awareness — Stay alert to security policies, requirements, procedures, and issues.

Employees should make a conscientious effort to avert security breaches by staying alert to potential vulnerabilities of House information and systems. Employees are in a position to see how security measures are truly used (or not used) and where potential problems exists. Certain human factors and activities may suggest that fraud or negligence may occur within the organization.

HIR will develop various forms of security training and awareness methods that will be available to all users. Users are also called on to stay abreast of current security information. It is an undisputed fact that an organization's strongest security measure is knowledgeable users.

It is recommended that employees:

- stay abreast of security policies, requirements, and issues,
- be alert to human factors that may indicate a security risk including:
    - employees with gambling or substance abuse problems,
    - employees who do not take leave as they are possible candidates for increased levels of stress or potential involvement in external coercion,
    - low morale,
    - poor relationships between management and staff.
- be alert to clues of abuse:
    - unauthorized computer products in the office (e.g., sports pools, personal business software),
    - possession of unauthorized equipment,
    - unscheduled programs running on a recurring basis.
- challenge unauthorized personnel in the work area,
- participate in security training as required,
- use security training programs and materials,
- read security information available to employees through Web pages, e-mail, newsletters, memos, and other sources,
- attend in-house workshops and exhibitions,
- talk with security officials (i.e., HIR Information Systems Security staff, Capitol Police, etc.).

Reporting	**Report security violations, incidents, and vulnerabilities to proper authorities.**

It is each employee's responsibility to report any form of security violations in accordance with in-office policy. It is important that the HIR Information Systems Security Office be contacted in cases of computer-related emergencies and violations so that action can be taken immediately to contain the exposure and minimize the impact on the rest of the House. Violations include non-compliance with established in-office procedures as well as approved House policies. In cases where laws may have been broken, employing authorities should also take action to contact law enforcement.

Employees must:

- ♦ report security vulnerabilities and violations as quickly as possible to proper authorities so that corrective action can be taken,
- ♦ report emergency incidents to the HIR Information Systems Security Office,
- ♦ take reasonable action (e.g., isolate equipment involved and do not use it until it has been analyzed) immediately upon discovering a violation to prevent additional damage,
- ♦ cooperate willingly with official action plans for dealing with security violations.

3.2 Principles of Behavior for Special Circumstances

The principles below apply to users in special circumstances. They are meant to provide extra guidance focused on specific situations where users have especially high responsibility for information security. Users addressed below include:

- ***privileged users***, which includes those with special access privileges for system development, delivery, and administration,
- ***World Wide Web privileged users***, which includes those with access privileges to maintain or update House web sites,
- ***users in procurement organizations***, who have access to sensitive information,
- ***authorized telecommuting personnel,***
- ***work from home*** and other ***remote users***,
- ***users of public access systems***, particularly the Internet,
- ***managers***, including information system and office managers,
- ***security personnel*** responsible for the security of House systems,
- ***contractors*** that provide services in support of House information systems.

A summary of principles of behavior for these special users and circumstances follows.

Principles of Behavior for Special Circumstances – User Responsibilities

Privileged Users	Privileged users must perform their duties meticulously and reliably in order to preserve information security.
World Wide Web Privileged Users	World Wide Web privileged users must ensure that information placed on a House web site is accurate, approved for public release, and protected against unauthorized modification.
Users in Procurement Organizations	Users in procurement organizations must apply all ethical and legal standards of procurement to their use of information systems.
Telecommuting Personnel, Users Working from Home, and Other Remote Users	Telecommuting and remote personnel must comply with all House policies and procedures to ensure continued protection of House information.
Administrators of Public Access Systems	Users must conduct only legitimate business through public access systems according to authorized procedures.
Managers	Managers must serve as leaders in information security by establishing a culture of awareness, ethical standards, and responsibility.
Security Personnel	Security personnel are responsible for evaluating and implementing the technical and procedural solutions for securing new and existing House systems.
Contractors	Contractors must adhere to the same standards and rules of conduct as House employees.

The following section discusses each special principle and lists practical means of implementing each principle.

Privileged Users

Privileged users include, but are not limited to:

- system administrators,
- authorized telecommuting personnel,
- computer operators,
- system engineers (those with control of the operating system),
- network administrators,
- security personnel,
- those who have access to change control parameters for equipment and software,
- data base administrators,
- those who control user passwords and access levels,
- troubleshooters/system maintenance and contractor personnel,
- contractors/vendors that perform system administration functions.

Privileged users of information systems must assume a high level of responsibility and initiative for security. With special skills and access rights, privileged users could, through negligence or malicious behavior, wreak havoc on a system. It is critical that they adhere to high ethical standards. Each office should maintain approved methods for each employing authority to gain access to supervisor/privileged passwords. Privileged users must use passwords that are a minimum of eight characters in length, as described in the Password Section of this document.

Privileged users are expected to take initiative in protecting against errors, abuse, theft, and sabotage.

Privileged users must make an effort to notice the threats to and vulnerabilities of information systems, calling these to the attention of management and working to develop effective countermeasures.

Privileged user responsibilities:

- ♦ perform their duties meticulously and reliably in order to preserve information security**,** integrity, availability, and confidentiality,

- ♦ use special access privileges only when they are needed to carry out a specific system function (whenever possible, use a non-privileged account),

- ♦ restrict access to all shared drives, directories, and other accessible resources to authorized users only,

- ♦ construct complex passwords that are a minimum of eight characters in length,

- ♦ use utility programs or operating system settings that will force users to construct strong passwords,

- ♦ implement a logon Warning Banner, as described in House guidance, notifying individuals that House systems are to be used for official business only, unauthorized system usage may violate House rules or United States Code, and disciplinary sanctions could result from unauthorized actions,

- protect the supervisor or administrator password at the highest level possible,
- help train users on appropriate use and security of the system,
- be aware of and monitor users who have responsibility for several functions (data entry, analysis, backups, output, etc.) that could potentially lead to abuse,
- report all security incidents to the appropriate authority,
- ensure virus protection is in place, functional, and current,
- never use information resources for personal business or gain,
- never gain access to data for the purpose of unauthorized copying, modification, deletion, and general viewing,
- use precautionary procedures and technical measures to protect privileged accounts from fraudulent use,
- watch for signs of hacker activity or other attempts at unauthorized access, such as multiple failed login attempts,
- review audit logs on a routine basis, at least weekly,
- watch for unauthorized use of information resources, including the presence of unauthorized software and data,
- take appropriate action to reduce damage from security violations, such as disconnecting a PC with a virus from the network or disabling a suspicious user account,
- alert the appropriate personnel when a system goes down or experiences problems,
- assist with recovery activities,
- be aware of the security requirements of their specific system and install software patches, etc. as appropriate,
- sign HISFORM-008.0, Affirmation of Non-Disclosure.

World Wide Web Privileged Users

World Wide Web (WWW) privileged users are those with permission to update and maintain House web sites.

WWW privileged users must assume a high level of responsibility for security. With special skills and access rights, WWW privileged users could, through negligence or malicious behavior post inaccurate, untrue, or confidential information to the WWW. These privileged users are expected to take initiative in protecting information against errors and sabotage.

WWW privileged user responsibilities:

- perform their duties reliably in order to preserve information accuracy and security,
- use special access privileges only when they are needed to carry out a specific system function,
- use a user account that is unique to each individual,
- report all security incidents to the appropriate authority,
- never use information resources for personal business or gain,
- never gain access to data for the purpose of unauthorized copying, modification, deletion, and general viewing,
- use precautionary procedures and technical measures to protect their privileged account from fraudulent use,
- watch for unauthorized use of information resources, including the presence of unauthorized information posted to a House web site,
- alert the appropriate personnel when a web site goes down or experiences problems,
- assist with recovery activities,
- sign HISFORM-008.0, Affirmation of Non-Disclosure.

Users in Procurement Organizations

Part of the job of employees in procurement organizations is daily use of confidentially sensitive information. Specifically, procurement-sensitive information is information about the House's plans and activities related to individual procurements. Employees involved in procurements also use ***Confidential Business Information (CBI)***, ***Confidential House Information (CHI),*** and other budgetary information extensively. Disclosure or misuse of such information can cause devastating losses and/or embarrassment to the House. Employees must adhere to ethical, procedural, and technical guidelines to safeguard confidentially sensitive information.

Employees must neither misuse nor knowingly disclose procurement-sensitive information. House Procurement Guidelines prohibit employees from using procurement sensitive information for one's own or another person's gain. For example, if in reviewing a proposal, an employee learned of a company's plans to introduce an innovative new product, the employee must not invest in the company on that basis. The employee also should not advise others to invest in that company.

The employee's duty to protect procurement-sensitive information continues when he/she changes position or leaves the House. Only when information has been declared public is an employee justified in disclosing it.

Users in procurement organizations must:

- abide by House and CAO Procurement Guidelines and Instructions,
- apply all ethical and legal standards of procurement to their use of information resources,
- as needed, seek the counsel of an ethics official or security officer,
- not disclose procurement-sensitive information,
- not use procurement-sensitive information for personal gain,
- not endorse products, services, or enterprises related to a procurement,
- not provide information about a vendor to another vendor,
- provide all vendors with equivalent information,
- avoid partiality and the appearance of partiality,
- not offer advice to outside parties based on knowledge of procurement-sensitive information.

Telecommuting Personnel, Users Working from Home, and Other Remote Users

The House has committed to providing a secure means for accomplishing work from a remote location. House employees utilize computers when they travel or need to accomplish work remotely after normal business hours. A higher level of responsibility for information security lies with remote users because the employee works unobserved, and the work environment falls outside the physical protection of a House facility.

Telecommuting is a working arrangement, mutually agreed upon by the employee and the House Office, whereby the employee works at an alternative work site on specified

days or during specified hours. Such remote users must establish a standard of self-discipline and initiative that ensures secure use of information resources. This means staying up-to- date on all House security policies concerning remote access.

Virtual Private Network (VPN) Users:

The House provides a Virtual Private Network (VPN) service for single-person District Offices, telecommuters, and House staff to access the House Network via House-owned PCs and laptops using their high-speed connections, SecurID cards and the Internet. Secure use of this service requires the following three security measures:

- Current anti-virus software must be installed on the system and operational at all times,
- A secure authentication device (SecurID card) must be used to access the House network,
- A personal firewall supported by the House VPN solution must be installed on the system and operational at the time of each connection to the House network.

Remote users must:

- ensure that adequate security provisions are implemented in the remote work environment to protect hardware, software, information, and infrastructure,
- use special measures to protect information and access capabilities across dial-up lines, such as changing passwords often and using an authentication device for a secure connection. Approved remote access authentication devices are provided by the HIR Information Systems Security Office,
- be alert for anomalies and vulnerabilities and report security incidents to authorities,
- disconnect or deactivate modems when they are not in use,
- accept only access to House systems which are necessary to perform their job,
- must use a current version of an anti-virus program,
- if using personal computer equipment to perform House-related work, use House provided shared resources – not a local computer device – to save information.

It is recommended that remote users:

- establish a thorough understanding and agreement with supervisors regarding appropriate security responsibilities,
- avoid uploading and downloading sensitive information,
- encrypt information when it is reasonable and worthwhile.

Administrators of Public Access Systems

Information security for public access systems, such as the Internet, is problematic and requires diligent monitoring. Intruders can get passwords and steal Internet Protocol (IP) addresses. Caution must be exercised to ensure security of House data.

Users must remember that publicly available information portrays the House image to the public. Much of the information placed on House public access systems represents House policy and positions, and such information must reflect high standards of integrity. Users must be careful to avoid the appearance of favoritism to or endorsement of any commercial entity**.**

Users must:

- adhere to all House information system polices and procedures,
- conduct only legitimate business through public access systems according to authorized procedures,
- use public access systems in accordance with an in-office policy,
- place only appropriate authorized information on a public access system, (Do not place prohibited, personal, or unofficial information on a World Wide Web (web) page on the Internet, send it via E-mail, nor enter it in a news group,
- not distribute or receive information in violation of copyright laws.

It is recommended that users:

- not allow sensitive information to be sent, received, or accessed through public access systems without proper precautions (e.g., encryption). Do not place segments of information on public access systems that could be pieced together to infer confidentially sensitive information,
- when maintaining e-mail and FAX distribution lists:
    - include only those who need and want the information,
    - update distribution lists as frequently as needed, but review at least annually,
    - process changes to e-mail users through the House Central Mail Directory.

Managers

Managers can strengthen information security through the culture they promote within their organizations. By following good security practices themselves, managers set an

example for employees. Managers must keep their knowledge of security issues and policies up-to-date so that they can counsel employees. Ethical practices must be the expected norm.

Managers must be alert to vulnerabilities and violations within their organizations. They must be aware of employees with personal problems, such as substance abuse, financial difficulties, or poor relationships with co-workers. When these problems exist, fraud, waste, and negligence are more likely to occur.

Managers must set up their organizational structure and procedures so that everyone is accountable for his/her actions. Otherwise, security breaches will be difficult to detect, correct, and prevent from recurring. The manager is accountable for the activities of the organization as a whole. Two key concepts are important: least privilege and separation of duties. Both of these limit the scope of individual users' functions, making it easier to track their actions.

Manager responsibilities:

- ♦ serve as leaders in information security by establishing a culture of awareness, ethical standards, and responsibility,
- ♦ take ownership of the employees actions and their responsibilities,
- ♦ emphasize information security as a priority issue with employees,
- ♦ encourage employees to take advantage of security training programs and materials,
- ♦ establish information accountability within the organization, such as manual and automated transaction logs,
- ♦ establish means of detecting thefts and abuses of information resources,
- ♦ be alert to threats and vulnerabilities of information and information systems, including personal and morale problems,
- ♦ initiate action to rectify security vulnerabilities and violations,
- ♦ record, investigate, and resolve all security violations in addition to reporting them to appropriate security officials,
- ♦ when an employee terminates or changes status, take the following actions:
    - notify the proper authorities (i.e., security personnel, if applicable and system administrators),
    - retrieve passwords and user IDs,
    - retrieve keys to encrypted files,
    - find out where information is stored and how to access it,
    - retrieve physical keys, badges, and SecurID cards (used for remote access),

- obtain documentation and direction on how to perform tasks,
- remind the employee of his/her duty to protect confidentially sensitive information from unauthorized disclosure.

♦ with friendly terminations, follow an orderly process that guarantees continued availability of the employee's information,

♦ with an unfriendly termination take the following quick action to prevent any possible sabotage:

- immediately terminate the employee's access to information and equipment,
- physical removal of the employee may be in order.

♦ ensure compliance with security obligations set forth in these guidelines for all contractor access to CBI or CHI.

Security Personnel

Security personnel are responsible to ensure that new and existing systems have a reasonable measure of security including:

♦ Confidentiality - the prevention of unauthorized disclosure of information,

♦ Integrity - the prevention of unauthorized modification of information,

♦ Availability - the prevention of unauthorized withholding of information or resources.

Security personnel are also responsible for:

♦ following new and changing trends in information security,

♦ developing policies and procedures for all House systems that require information security,

♦ testing the effectiveness of policies, procedures, and technical security solutions on a continuous basis,

♦ assisting all employees with the secure use of House systems.

Contractors

Contractors are expected, to follow the same standards and rules of conduct with regard to the support of House information systems as House employees. Contractor personnel may perform in the same capacity as House system personnel and as such must adhere to the guidelines contained herein. Additionally, all contracts will explicitly state that Contractor personnel:

- must be eligible for a Federal government security clearance if access to Confidential Business Information or Confidential House Information is required.* Individual House Offices or CAO Business Units may require an Office of Personnel (OPM) Extended Background Investigation or other security clearance, as deemed necessary,

- must not remove Confidential Business Information or Confidential House Information from the Capitol campus,

- must sign the HISFORM-008.0, **Affirmation of Non-Disclosure** prior to conducting House business.

*Upon written request, the CAO HIR Information Systems Security Office can grant exceptions to this requirement when access to House information is limited in scope and contract duration, and when the employing office proposes sufficient compensating controls to protect House information. Written requests should address the specific circumstances, the rational for the exception, compensating controls, and the resulting risk to House information.

4.0 IMPLEMENTING GENERAL INFORMATION SECURITY GUIDELINES

4.1 Integrating General Information Security Guidelines into Security Planning

Good business practice mandates that General Information Security Guidelines become part of the security plan for general support systems and major applications. Guidelines must be in a separate area and must address:

- responsibilities and expectations of all users with access to the system,

- consequences for non-compliance.

4.2 Integrating Guidelines into Training

Employees should familiarize themselves on General Information Security Guidelines before they access a House system. General Information Security Guidelines will be included as part of initial system training in order to reduce security violations. Users trained in ethical standards and technical procedures are the strongest part of the information security program. Most people want to do the right thing. As long as they understand why they are asked to do things, they will usually strive to do them. On the other hand, users not aware of the implications of negligence, for example, may very well circumvent rules in an effort to get their jobs done efficiently. Trained users know what is required and why, and will be much more likely to act responsibly and expect others to act responsibly.

Offices must keep appropriate records and institute a process of security training that users must complete before being granted access to systems, and periodically thereafter. House Information Resources (HIR) will continue to provide guidance to offices through various information security awareness training.

4.3 Addressing Individual System Requirements

Each office may have its own unique General Information Security Guidelines. Each should address all the applicable principles set forth in this document. The list of General Information Security Guidelines in this document provide the building block.

For an existing system, the rules must correspond with existing technical security controls. For example, a system is set with certain account types; a corresponding rule would state that users must access only the account type(s) granted them, without attempting to gain higher access through illicit actions such as hacking the network or using someone else's account. Those who write the General Information Security Guidelines must consider the intent behind each technical control, and write the corresponding rule to state that intent.

4.4 Consequences of Non-Compliance

Non-compliance with any element of this House Information Security Policy may subject the violator to appropriate disciplinary action including but not limited to the following:

- suspension of access privileges,
- warning (verbal or written),
- reprimand,
- suspension from employment,
- demotion from job position,
- termination of employment,
- financial liability for actual, consequential and incidental damages,
- criminal and civil penalties, including prison terms and fines.

The listed disciplinary actions are merely suggestions that can be used depending on the severity of the violation. This list is not exhaustive and does not imply that disciplinary actions are mandatory. It is within each employing authority's discretion to determine appropriate disciplinary measures under each circumstance. However, under the scope of House Rules and Committee on Standards of Official Conduct jurisdiction, certain violations may result in action by the House.

The consequences on non-compliance should be fully disclosed to all users and each user should sign an acknowledgement that the user has received, understands and agrees to abide by the guidelines (policies).